THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

SCOTT WEISCOPE, on behalf of himself and all others similarly situated, Plaintiff, v. RESOURCE ANESTHESIOLOGY ASSOCIATES OF IL, P.C. and SOMNIA, INC., Defendants.	Case No.: **CLASS ACTION COMPLAINT** DEMAND FOR JURY TRIAL

Plaintiff Scott Weiscope ("Plaintiff") brings this Class Action Complaint against Resource Anesthesiology Associates of IL, P.C. ("RAAI") and Somnia, Inc. ("Somnia") (collectively, "Defendants"), individually and on behalf of all others similarly situated ("Class Members"), and alleges, upon personal knowledge as to his own actions and his counsels' investigations, and upon information and belief as to all other matters, as follows:

I. INTRODUCTION

1. Plaintiff brings this class action against Defendants for their failure to properly secure and safeguard personal identifiable information ("PII")[1] and protected health information ("PHI") for more than one hundred thousand individuals who received services from Defendants or their affiliates, including, but not limited to, name, date of birth, driver's license number,

[1] Personally identifiable information generally incorporates information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information. 2 C.F.R. § 200.79. At a minimum, it includes all information that on its face expressly identifies an individual.

financial account information, health insurance policy number, Medical Record Number, Medicaid or Medicare ID, and health information such as treatment and diagnosis info.

2. According to Somnia's website, it is "a practice management company singularly focused on anesthesiology."[2]

3. RAAI is one of several anesthesiology practices that uses Somnia for practice management and to which Somnia provides administrative services.

4. Prior to and through July 11, 2022, Somnia obtained from RAAI and other anesthesiology practices the PII and PHI of Plaintiff and Class Members and stored that PII and PHI, unencrypted, in an Internet-accessible environment on Somnia's network.

5. On or around September 22, 2022, RAAI learned from Somnia of suspicious activity that impacted Somnia's ability to access some of its systems, during which information about patients of RAAI and other anesthesiology practices may have been compromised, including date of birth, driver's license number, financial account information, health insurance policy number, Medical Record Number, Medicaid or Medicare ID, and health information such as treatment and diagnosis info, (the "Data Breach").

6. Somnia determined that the files and folders removed during the Data Breach contained the PII and PHI of more than 100,000 individuals who obtained services from Defendants and their affiliates, including Plaintiff and Class Members.

7. On or around October 24, 2022, Defendants and their affiliates began notifying various states Attorneys General of the Data Breach.

8. On or around October 24, 2022, Defendants and their affiliates began notifying Plaintiff and Class Members of the Data Breach.

[2] *See* https://somniaanesthesiaservices.com/somnia-anesthesia/ (last visited Nov. 7, 2022).

9. By obtaining, collecting, using, and deriving a benefit from the PII and PHI of Plaintiff and Class Members, Defendants assumed legal and equitable duties to those individuals to protect and safeguard that information from unauthorized access and intrusion. Defendants admit that the unencrypted PII and PHI exposed to "unauthorized activity" included name, date of birth, driver's license number, financial account information, health insurance policy number, Medical Record Number, Medicaid or Medicare ID, and health information such as treatment and diagnosis info.

10. The exposed PII and PHI of Plaintiff and Class Members can be sold on the dark web. Hackers can access and then offer for sale the unencrypted, unredacted PII and PHI to criminals. Plaintiff and Class Members now face a lifetime risk of (i) identity theft, which is heightened here by the loss of Social Security numbers, and (ii) the sharing and detrimental use of their confidential medical information.

11. The PII and PHI were compromised due to Defendants' negligent and/or careless acts and omissions and the failure to protect the PII and PHI of Plaintiff and Class Members. In addition to Defendants' failure to prevent the Data Breach, Defendants waited several months after the Data Breach occurred to report it to the states' Attorneys General and affected individuals. Defendants have also purposefully maintained secret the specific vulnerabilities and root causes of the breach and has not informed Plaintiff and Class Members of that information.

12. As a result of this delayed response, Plaintiff and Class Members had no idea their PII and PHI had been compromised, and that they were, and continue to be, at significant risk of identity theft and various other forms of personal, social, and financial harm, including the sharing and detrimental use of their confidential medical information. The risk will remain for their respective lifetimes.

13. Plaintiff brings this action on behalf of all persons whose PII and PHI was compromised as a result of Defendants' failure to: (i) adequately protect the PII and PHI of Plaintiff and Class Members; (ii) warn Plaintiff and Class Members of Defendants' inadequate information security practices; and (iii) effectively secure hardware containing protected PII and PHI using reasonable and effective security procedures free of vulnerabilities and incidents. Defendants' conduct amounts to negligence and violates federal and state statutes.

14. Plaintiff and Class Members have suffered injury as a result of Defendants' conduct. These injuries include: (i) lost or diminished value of PII and PHI; (ii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII and PHI; (iii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time, (iv) the disclosure of their private information, including medical information, and (v) the continued and certainly increased risk to their PII and PHI, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) may remain backed up in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII and PHI.

15. Defendants disregarded the rights of Plaintiff and Class Members by intentionally, willfully, recklessly, or negligently failing to take and implement adequate and reasonable measures to ensure that the PII and PHI of Plaintiff and Class Members was safeguarded, failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required and appropriate protocols, policies and procedures regarding the encryption of data, even for internal use. As the result, the PII and PHI of Plaintiff and Class Members was compromised through disclosure to an unknown and unauthorized third party. Plaintiff and Class

Members have a continuing interest in ensuring that their information is and remains safe, and they should be entitled to injunctive and other equitable relief.

II. PARTIES

16. Plaintiff Scott Weiscope is a Citizen of Illinois residing in Mattoon, Illinois.

17. RAAI is a corporation organized under the laws of Illinois with a principal place of business in Chicago, Illinois.

18. Somnia is a corporation organized under the laws of New York with a principal place of business in Harrison, New York.

19. The true names and capacities of persons or entities, whether individual, corporate, associate, or otherwise, who may be responsible for some of the claims alleged herein are currently unknown to Plaintiff. Plaintiff will seek leave of court to amend this complaint to reflect the true names and capacities of such other responsible parties when their identities become known.

20. All of Plaintiff's claims stated herein are asserted against Defendants and any of their owners, predecessors, successors, subsidiaries, agents and/or assigns.

III. JURISDICTION AND VENUE

21. This Court has subject matter and diversity jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action wherein the amount of controversy exceeds the sum or value of $5 million, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one Class Member is a citizen of a state different from Defendants to establish minimal diversity.

22. RAAI is a citizen of Illinois because it is an Illinois corporation with a principal place of business in Illinois.

23. Somnia is a citizen of New York because it is a New York corporation with a principal place of business in New York.

24. The Southern District of New York has personal jurisdiction over RAAI because entrusted Plaintiff's PII and PHI to Somnia in New York.

25. The Southern District of New York has personal jurisdiction over Somnia because it conducts substantial business in New York and this District.

26. Venue is proper in this District under 28 U.S.C. §1391(b) because Somnia operates in this District, RAAI provided and entrusted Plaintiff's PII and PHI to Somnia in this District, and a substantial part of the events or omissions giving rise to Plaintiff's claims occurred in this District.

IV. FACTUAL ALLEGATIONS

Background

27. Plaintiff and Class Members, who obtained services from Defendants or their affiliates, provided and entrusted Defendants with sensitive and confidential information, including name, date of birth, driver's license number, financial account information, health insurance policy number, Medical Record Number, Medicaid or Medicare ID, and health information such as treatment and diagnosis info.

28. Plaintiff and Class Members relied on these sophisticated Defendants to keep their PII and PHI confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information. Plaintiff and Class Members demand security to safeguard their PII and PHI.

29. Defendants had a duty to adopt reasonable measures to protect the PII and PHI of Plaintiff and Class Members from involuntary disclosure to third parties.

The Data Breach

30. On or about October 24, 2022, Defendants and their affiliates sent Plaintiff and Class Members a *Notice of Data Security Incident* in substantially the same form.[3] Defendants and their affiliates informed Plaintiff and Class Members that:

> On September 22, 2022, <<Variable Text 1>> learned from its management company of suspicious activity that impacted the management company's ability access to some of its systems. The management company provides administrative services to the <<Variable Text 1>> and may have your protected health information stored on its systems in the performance of these services.
>
> **What Happened?**
>
> On July 11, 2022, <<Variable Text 1>>'s management company identified suspicious activity on its systems. The management company immediately implemented its incident response protocols, disconnected all systems, and engaged external cybersecurity experts to conduct a forensic investigation. The investigation found that some information stored on the management company's systems may have been compromised. The management company then reviewed the potentially impacted information to identify any protected health information that may have been affected. This review was recently completed, at which point we determined that your protected health information have been affected.
>
> **What Information Was Involved?**
>
> Impacted information may include your name, Social Security number, and some combination of the following data elements: date of birth, driver's license number, financial account information, health insurance policy number, Medical Record Number, Medicaid or Medicare ID, and health information such as treatment and diagnosis info.[4]

31. On or about October 24, 2022, Defendants and their affiliates notified various state

[3] Exhibit 1 (sample notice filed with Montana attorney general's office), *available at* https://media.dojmt.gov/wp-content/uploads/Consumer-Notification-Letter-640.pdf (last visited Nov. 7, 2022).

[4] *Id.*

Attorneys General of the Data Breach and provided them "sample" notices of the Data Breach.

32. On or about October 24, 2022, Defendants and their affiliates notified the United States Department of Health and Human Services that 18,321 patients of RAAI were impacted by the Data Breach and more than 100,000 individuals in total were impacted by the Data Breach.

33. Defendants admitted in the *Notice of Data Security Incident*, the letters to the Attorneys General, and the "sample" notices of the Data Breach that Plaintiff's and Class Members' PII and PHI may have been compromised, including date of birth, driver's license number, financial account information, health insurance policy number, Medical Record Number, Medicaid or Medicare ID, and health information such as treatment and diagnosis info.

34. In response to the Data Breach, Defendants claim that "[t]he management company has assured us that they have taken steps to prevent a similar incident in the future, including conducting a global password reset, tightening firewall restrictions, and implementing endpoint threat detection and response monitoring software on workstations and servers..."[5] However, the details of the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure a breach does not occur again have not been shared with regulators or Plaintiff and Class Members, who retain a vested interest in ensuring that their information remains protected.

35. The unencrypted PII and PHI of Plaintiff and Class Members may end up for sale on the dark web, or simply fall into the hands of companies that will use the detailed PII and PHI for targeted marketing without the approval of Plaintiff and Class Members. Unauthorized individuals can easily access the PII and PHI of Plaintiff and Class Members.

36. Defendants did not use reasonable security procedures and practices appropriate to

[5] *Id.*

the nature of the sensitive, unencrypted information they were maintaining for Plaintiff and Class Members, causing the exposure of PII and PHI for more than 100,000 individuals.

37. Because Defendants had a duty to protect Plaintiff's and Class Members' PII and PHI, Defendants should have accessed readily available and accessible information about potential threats for the unauthorized exfiltration and misuse of such information.

38. In the years immediately preceding the Data Breach, Defendants knew or should have known that Defendants' computer systems were a target for cybersecurity attacks, including ransomware attacks involving data theft, because warnings were readily available and accessible via the internet.

39. In October 2019, the Federal Bureau of Investigation published online an article titled "High-Impact Ransomware Attacks Threaten U.S. Businesses and Organizations" that, among other things, warned that "[a]lthough state and local governments have been particularly visible targets for ransomware attacks, ***ransomware actors have also targeted health care organizations***, ***industrial companies***, and the transportation sector."[6]

40. In April 2020, ZDNet reported, in an article titled "Ransomware mentioned in 1,000+ SEC filings over the past year," that "***[r]ansomware gangs are now ferociously aggressive in their pursuit of big companies***. They breach networks, use specialized tools to maximize damage, ***leak corporate information on dark web portals***, and even tip journalists to generate negative news for companies as revenge against those who refuse to pay."[7]

---

[6] FBI, High-Impact Ransomware Attacks Threaten U.S. Businesses and Organizations (Oct. 2, 2019) (emphasis added), *available at* https://www.ic3.gov/Media/Y2019/PSA191002 (last visited Jan. 25, 2022).

[7] ZDNet, Ransomware mentioned in 1,000+ SEC filings over the past year (Apr. 30, 2020) (emphasis added), *available at* https://www.zdnet.com/article/ransomware-mentioned-in-1000-sec-filings-over-the-past-year/ (last visited Jan. 25, 2022).

41. In September 2020, the United States Cybersecurity and Infrastructure Security Agency published online a "Ransomware Guide" advising that ***"[m]alicious actors have adjusted their ransomware tactics over time to include pressuring victims for payment by threatening to release stolen data*** if they refuse to pay and publicly naming and shaming victims as secondary forms of extortion."[8]

42. This readily available and accessible information confirms that, prior to the Data Breach, Defendants knew or should have known that (i) ransomware actors were targeting healthcare companies such as Defendants, (ii) ransomware gangs were ferociously aggressive in their pursuit of big companies such as Defendants, (iii) ransomware gangs were leaking corporate information on dark web portals, and (iv) ransomware tactics included threatening to release stolen data.

43. In light of the information readily available and accessible on the internet before the Data Breach, Defendants, having elected to store the unencrypted PII and PHI of more than 100,000 individuals in an Internet-accessible environment, had reason to be on guard for the exfiltration of the PII and PHI and Defendants' type of business had cause to be particularly on guard against such an attack.

44. Prior to the Data Breach, Defendants knew or should have known that there was a foreseeable risk that Plaintiff's and Class Members' PII and PHI could be accessed, exfiltrated, and published as the result of a cyberattack.

45. Prior to the Data Breach, Defendants knew or should have known that they should have encrypted the Social Security numbers and other sensitive data elements within the PII and

[8] U.S. CISA, Ransomware Guide – September 2020, *available at* https://www.cisa.gov/sites/default/files/publications/CISA_MS ISAC_Ransomware%20Guide_S508C_.pdf (last visited Jan. 25, 2022).

PHI to protect against their publication and misuse in the event of a cyberattack.

Defendants Acquire, Collect, and Store the PII and PHI of Plaintiff and Class Members.

46. As a condition of obtaining services from, Defendants required that Plaintiff and Class Members entrust Defendants with highly confidential PII and PHI.

47. Defendants acquired, collected, and stored the PII and PHI of Plaintiff and Class Members.

48. By obtaining, collecting, and storing the PII and PHI of Plaintiff and Class Members, Defendants assumed legal and equitable duties and knew or should have known that they were responsible for protecting the PII and PHI from disclosure.

49. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their PII and PHI and relied on Defendants to keep their PII and PHI confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

50. As explained by the Federal Bureau of Investigation, "[p]revention is the most effective defense against ransomware and it is critical to take precautions for protection."[9]

51. To prevent and detect ransomware attacks, including the ransomware attack that resulted in the Data Breach, Defendants could and should have implemented, as recommended by the United States Government, the following measures:

- Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.
- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF),

[9] *See* How to Protect Your Networks from RANSOMWARE, at 3, *available at* https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view (last visited Aug. 23, 2021).

Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.

- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.
- Configure firewalls to block access to known malicious IP addresses.
- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.
- Set anti-virus and anti-malware programs to conduct regular scans automatically.
- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.
- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.
- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.
- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.
- Consider disabling Remote Desktop protocol (RDP) if it is not being used.
- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.
- Execute operating system environments or specific programs in a virtualized environment.
- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.[10]

52. To prevent and detect ransomware attacks, including the ransomware attack that resulted in the Data Breach, Defendants could and should have implemented, as recommended by

[10] *Id.* at 3-4.

the United States Cybersecurity & Infrastructure Security Agency, the following measures:

- **Update and patch your computer**. Ensure your applications and operating systems (OSs) have been updated with the latest patches. Vulnerable applications and OSs are the target of most ransomware attacks….

- **Use caution with links and when entering website addresses**. Be careful when clicking directly on links in emails, even if the sender appears to be someone you know. Attempt to independently verify website addresses (e.g., contact your organization's helpdesk, search the internet for the sender organization's website or the topic mentioned in the email). Pay attention to the website addresses you click on, as well as those you enter yourself. Malicious website addresses often appear almost identical to legitimate sites, often using a slight variation in spelling or a different domain (e.g., .com instead of .net)….

- **Open email attachments with caution**. Be wary of opening email attachments, even from senders you think you know, particularly when attachments are compressed files or ZIP files.

- **Keep your personal information safe**. Check a website's security to ensure the information you submit is encrypted before you provide it….

- **Verify email senders**. If you are unsure whether or not an email is legitimate, try to verify the email's legitimacy by contacting the sender directly. Do not click on any links in the email. If possible, use a previous (legitimate) email to ensure the contact information you have for the sender is authentic before you contact them.

- **Inform yourself**. Keep yourself informed about recent cybersecurity threats and up to date on ransomware techniques. You can find information about known phishing attacks on the Anti-Phishing Working Group website. You may also want to sign up for CISA product notifications, which will alert you when a new Alert, Analysis Report, Bulletin, Current Activity, or Tip has been published.

- **Use and maintain preventative software programs**. Install antivirus software, firewalls, and email filters—and keep them updated—to reduce malicious network traffic….[11]

53. To prevent and detect ransomware attacks, including the ransomware attack that resulted in the Data Breach, Defendants could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

[11] *See* Security Tip (ST19-001) Protecting Against Ransomware (original release date Apr. 11, 2019), *available at* https://us-cert.cisa.gov/ncas/tips/ST19-001 (last visited Aug. 23, 2021).

Secure internet-facing assets

- Apply latest security updates
- Use threat and vulnerability management
- Perform regular audit; remove privileged credentials;

Thoroughly investigate and remediate alerts

- Prioritize and treat commodity malware infections as potential full compromise;

Include IT Pros in security discussions

- Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely;

Build credential hygiene

- Use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords

Apply principle of least-privilege

- Monitor for adversarial activities
- Hunt for brute force attempts
- Monitor for cleanup of Event Logs
- Analyze logon events

Harden infrastructure

- Use Windows Defender Firewall
- Enable tamper protection
- Enable cloud-delivered protection
- Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office [Visual Basic for Applications].[12]

54. Given that Defendants were storing the PII and PHI of more than 18,000 (RAAI) and 100,000 (Somnia) individuals, Defendants could and should have implemented all of the above

[12] *See* Human-operated ransomware attacks: A preventable disaster (Mar 5, 2020), *available at* https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/ (last visited Aug. 23, 2021).

measures to prevent and detect ransomware attacks.

55. The occurrence of the Data Breach indicates that Defendants failed to adequately implement one or more of the above measures to prevent ransomware attacks, resulting in the Data Breach and the exposure of the PII and PHI of more than 100,000 individuals, including Plaintiffs and Class Members.

Securing PII and PHI and Preventing Breaches

56. Defendants could have prevented this Data Breach by properly securing and encrypting the folders, files, and or data fields containing the PII and PHI of Plaintiff and Class Members. Alternatively, Defendants could have destroyed the data they no longer had a reasonable business need to maintain or only stored data in an Internet-accessible environment when there was a reasonable need to do so.

57. Defendants' negligence in safeguarding the PII and PHI of Plaintiff and Class Members is exacerbated by the repeated warnings and alerts directed to protecting and securing sensitive data.

58. Despite the prevalence of public announcements of data breach and data security compromises, Defendants failed to take appropriate steps to protect the PII and PHI of Plaintiff and Class Members from being compromised.

59. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[13] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's

[13] 17 C.F.R. § 248.201 (2013).

license or identification number, alien registration number, government passport number, employer or taxpayer identification number."[14]

60. The ramifications of Defendants' failure to keep secure the PII and PHI of Plaintiff and Class Members are long lasting and severe. Once PII and PHI is stolen, particularly Social Security numbers, fraudulent use of that information and damage to victims may continue for years.

Value of Personal Identifiable Information

61. The PII and PHI of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[15] Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web.[16] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[17]

62. Social Security numbers, for example, are among the worst kind of personal information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive

---

[14] *Id*.

[15] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, *available at*: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last accessed Jan. 26, 2022).

[16] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, *available at*: https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last accessed Jan. 26, 2022).

[17] *In the Dark*, VPNOverview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last accessed Dec. 29, 2020).

financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[18]

63. What is more, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

64. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "The credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[19]

65. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to

[18] Social Security Administration, *Identity Theft and Your Social Security Number*, *available at*: https://www.ssa.gov/pubs/EN-05-10064.pdf (last accessed Jan. 26, 2022).

[19] Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), *available at*: http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millionsworrying-about-identity-theft (last accessed Jan. 26, 2022).

change—Social Security number, driver's license or state identification number, and biometrics.

66. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market."[20]

67. Among other forms of fraud, identity thieves may obtain driver's licenses, government benefits, medical services, and housing or even give false information to police.

68. The fraudulent activity resulting from the Data Breach may not come to light for years.

69. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII and PHI is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[21]

70. At all relevant times, Defendants knew, or reasonably should have known, of the importance of safeguarding the PII and PHI of Plaintiff and Class Members, including Social Security numbers, and of the foreseeable consequences that would occur if Defendants' data

[20] Time Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), *available at*: https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last accessed Jan. 26, 2022).

[21] *Report to Congressional Requesters*, GAO, at 29 (June 2007), *available at:* https://www.gao.gov/assets/gao-07-737.pdf (last accessed Mar. 15, 2021).

security system was breached, including, specifically, the significant costs that would be imposed on Plaintiff and Class Members as a result of a breach.

71. Plaintiff and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their PII and PHI.

72. Defendants were, or should have been, fully aware of the unique type and the significant volume of data contained in Defendants' folders and files, amounting to potentially tens of thousands of individuals' detailed, personal information and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

73. To date, Defendants have offered Plaintiff and Class Members whose Social Security numbers were impacted only two years of credit monitoring and identity theft detection through IDX. The offered service is inadequate to protect Plaintiff and Class Members from the threats they face for years to come, particularly in light of the PII and PHI at issue here.

74. The injuries to Plaintiff and Class Members were directly and proximately caused by Defendants' failure to implement or maintain adequate data security measures for the PII and PHI of Plaintiff and Class Members.

Plaintiff's Experience

75. Prior to the Data Breach, Plaintiff obtained services from RAAI. As a condition of providing services to Plaintiff, RAAI required that he provide and entrust his PII and PHI.

76. Plaintiff received Defendants' *Notice of Data Security Incident*, dated October 24, 2022, on or about that date. The notice stated that Plaintiff's PII and PHI may have been compromised as a result of the Data Breach.

77. As a result of the Data Breach, Plaintiff's PII and PHI were potentially

compromised. The confidentiality of Plaintiff's PII and PHI has been irreparably harmed. For the rest of his life, Plaintiff will have to worry about when and how his PII and PHI may be shared or used to his detriment.

78. As a result of the Data Breach notice, Plaintiff spent time dealing with the consequences of the Data Breach, which includes time spent verifying the legitimacy of the Notice of Data Breach. This time has been lost forever and cannot be recaptured.

79. Additionally, Plaintiff is very careful about sharing his sensitive PII and PHI. He has never knowingly transmitted unencrypted sensitive PII and PHI over the internet or any other unsecured source.

80. Plaintiff stores any documents containing his sensitive PII and PHI in a safe and secure location or destroys the documents. Moreover, he diligently chooses unique usernames and passwords for his various online accounts.

81. Plaintiff suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of his privacy.

82. Plaintiff has suffered imminent and impending injury arising from the substantially increased risk misuse resulting from his PII and PHI being placed in the hands of unauthorized third parties and possibly criminals.

83. Plaintiff has a continuing interest in ensuring that his PII and PHI, which, upon information and belief, remains backed up in Defendants' possession, is protected and safeguarded from future breaches.

V. CLASS ALLEGATIONS

84. Plaintiff brings this nationwide class action on behalf of himself and on behalf of all others similarly situated pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules

of Civil Procedure.

85. The Nationwide Class that Plaintiff seeks to represent is defined as follows:

> All individuals whose PII and/or PHI was compromised or potentially compromised in the data breach that is the subject of the Notice of Data Security Incident that Defendants and their affiliates sent to Plaintiff and Class Members on or around October 24, 2022 (the "Nationwide Class").

86. Pursuant to Rule 23, and in the alternative to claims asserted on behalf of the Nationwide Class, Plaintiff asserts claims on behalf of a separate subclass, defined as follows:

> All individuals whose PII and/or PHI RAAI entrusted to Somnia and whose PII and/or PHI was compromised or potentially compromised in the data breach that is the subject of the Notice of Data Security Incident that RAAI sent to Plaintiff on or around October 24, 2022 (the "RAAI Subclass").

87. Excluded from the Class are the following individuals and/or entities: Defendants and Defendants' parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendants have a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state or local governments, including but not limited to their departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

88. Plaintiff reserves the right to modify or amend the definition of the proposed classes before the Court determines whether certification is appropriate.

89. Numerosity, Fed R. Civ. P. 23(a)(1): The Nationwide Class (the "Class") are so numerous that joinder of all members is impracticable. Defendants have identified tens of thousands of individuals whose PII and PHI was compromised in the Data Breach, and the Class is apparently identifiable within Defendants' records. Defendants advised the United States

Department of Health and Human Services that the Data Breach affected 18,321 patients of RAAI and more than 100,000 individuals in total.

90. Commonality, Fed. R. Civ. P. 23(a)(2) and (b)(3): Questions of law and fact common to the Classes exist and predominate over any questions affecting only individual Class Members. These include:

a. Whether and to what extent Defendants had a duty to protect the PII and PHI of Plaintiff and Class Members;

b. Whether Defendants had duties not to disclose the PII and PHI of Plaintiff and Class Members to unauthorized third parties;

c. Whether Defendants had duties not to use the PII and PHI of Plaintiff and Class Members for non-business purposes;

d. Whether Defendants failed to adequately safeguard the PII and PHI of Plaintiff and Class Members;

e. When Defendants actually learned of the Data Breach;

f. Whether Defendants adequately, promptly, and accurately informed Plaintiff and Class Members that their PII and PHI had been compromised;

g. Whether Defendants violated the law by failing to promptly notify Plaintiff and Class Members that their PII and PHI had been compromised;

h. Whether Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

i. Whether Defendants adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

j. Whether Defendants engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII and PHI of Plaintiff and Class Members;

k. Whether Plaintiff and Class Members are entitled to actual, consequential, and/or nominal damages as a result of Defendants' wrongful conduct;

l. Whether Plaintiff and Class Members are entitled to restitution as a result of Defendants' wrongful conduct; and

m. Whether Plaintiff and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

91. Typicality, Fed. R. Civ. P. 23(a)(3): Plaintiff's claims are typical of those of other Class Members because all had their PII and PHI compromised as a result of the Data Breach, due to Defendants' misfeasance.

92. Policies Generally Applicable to the Class: This class action is also appropriate for certification because Defendants have acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect to the Class as a whole. Defendants' policies challenged herein apply to and affect Class Members uniformly and Plaintiff's challenge of these policies hinges on Defendants' conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiff.

93. Adequacy, Fed. R. Civ. P. 23(a)(4): Plaintiff will fairly and adequately represent and protect the interests of the Class Members in that he has no disabling conflicts of interest that would be antagonistic to those of the other Members of the Class. Plaintiff seeks no relief that is antagonistic or adverse to the Members of the Class and the infringement of the rights and the damages they have suffered are typical of other Class Members. Plaintiff has retained counsel

experienced in complex class action litigation, and Plaintiff intends to prosecute this action vigorously.

94. Superiority and Manageability, Fed. R. Civ. P. 23(b)(3): The class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against large corporations, like Defendants. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

95. The nature of this action and the nature of laws available to Plaintiff and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiff and Class Members for the wrongs alleged because Defendants would necessarily gain an unconscionable advantage since it would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiff was exposed is representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

96. The litigation of the claims brought herein is manageable. Defendants' uniform

conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

97. Adequate notice can be given to Class Members directly using information maintained in Defendants' records.

98. Unless a Class-wide injunction is issued, Defendants may continue in their failure to properly secure the PII and PHI of Class Members, Defendants may continue to refuse to provide proper notification to Class Members regarding the Data Breach, and Defendants may continue to act unlawfully as set forth in this Complaint.

99. Further, Defendants have acted or refused to act on grounds generally applicable to the Classes and, accordingly, final injunctive or corresponding declaratory relief with regard to the Class Members as a whole is appropriate under Rule 23(b)(2) of the Federal Rules of Civil Procedure.

100. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendants owed a legal duty to Plaintiff and Class Members to exercise due care in collecting, storing, using, and safeguarding their PII and PHI;

b. Whether Defendants breached a legal duty to Plaintiff and Class Members to exercise due care in collecting, storing, using, and safeguarding their PII and PHI;

c. Whether Defendants failed to comply with their own policies and applicable laws, regulations, and industry standards relating to data security;

d. Whether an implied contract existed between Defendants on the one hand, and Plaintiff and Class Members on the other, and the terms of that implied contract;

e. Whether Defendants breached the implied contract;

f. Whether Defendants adequately and accurately informed Plaintiff and Class Members that their PII and PHI had been compromised;

g. Whether Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

h. Whether Defendants engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII and PHI of Plaintiff and Class Members; and,

i. Whether Class Members are entitled to actual, consequential, and/or nominal damages, and/or injunctive relief as a result of Defendants' wrongful conduct.

COUNT I
NEGLIGENCE
(On Behalf of Plaintiff and the Nationwide Class)

101. Plaintiff and the Nationwide Class re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 99.

102. As a condition of obtaining services from Defendants or their affiliates, Plaintiff and Class Members were obligated to provide and entrust Defendants or their affiliates with certain PII and PHI.

103. Plaintiff and the Nationwide Class provided and entrusted their PII and PHI to Defendants or their affiliates on the premise and with the understanding that Defendants would

safeguard their information, use their PII and PHI for business purposes only, and not disclose their PII and PHI to unauthorized third parties.

104. Defendants have full knowledge of the sensitivity of the PII and PHI and the types of harm that Plaintiff and the Nationwide Class could and would suffer if the PII and PHI were wrongfully disclosed.

105. Defendants knew or reasonably should have known that the failure to exercise due care in the collecting, storing, and using of the PII and PHI of Plaintiff and the Nationwide Class involved an unreasonable risk of harm to Plaintiff and the Nationwide Class, even if the harm occurred through the criminal acts of a third party.

106. Defendants had a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This duty includes, among other things, designing, maintaining, and testing Defendants' security protocols to ensure that the PII and PHI of Plaintiff and the Nationwide Class in Defendants' possession was adequately secured and protected.

107. Defendants also had a duty to exercise appropriate clearinghouse practices to remove from an Internet-accessible environment the PII and PHI they were no longer required to retain pursuant to regulations and had no reasonable business need to maintain in an Internet-accessible environment.

108. Defendants also had a duty to have procedures in place to detect and prevent the improper access and misuse of the PII and PHI of Plaintiff and the Nationwide Class.

109. Defendants' duty to use reasonable security measures arose as a result of the special relationship that existed between Defendants and Plaintiff and the Nationwide Class. That special relationship arose because Plaintiff and the Nationwide Class entrusted Defendants with their

confidential PII and PHI, a necessary part of obtaining services from Defendants or their affiliates.

110. Defendants were subject to an "independent duty," untethered to any contract between Defendants and Plaintiff or the Nationwide Class.

111. A breach of security, unauthorized access, and resulting injury to Plaintiff and the Nationwide Class was reasonably foreseeable, particularly in light of Defendants' inadequate security practices.

112. Plaintiff and the Nationwide Class were the foreseeable and probable victims of any inadequate security practices and procedures. Defendants knew or should have known of the inherent risks in collecting and storing the PII and PHI of Plaintiff and the Nationwide Class, the critical importance of providing adequate security of that PII and PHI, and the necessity for encrypting PII and PHI stored on Defendants' systems.

113. Defendants' own conduct created a foreseeable risk of harm to Plaintiff and the Nationwide Class. Defendants' misconduct included, but was not limited to, their failure to take the steps and opportunities to prevent the Data Breach as set forth herein. Defendants' misconduct also included their decisions not to comply with industry standards for the safekeeping of the PII and PHI of Plaintiff and the Nationwide Class, including basic encryption techniques freely available to Defendants.

114. Plaintiff and the Nationwide Class had no ability to protect their PII and PHI that was in, and possibly remains in, Defendants' possession.

115. Defendants were in a position to protect against the harm suffered by Plaintiff and the Nationwide Class as a result of the Data Breach.

116. Defendants had and continue to have a duty to adequately disclose that the PII and PHI of Plaintiff and the Nationwide Class within Defendants' possession might have been

compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was necessary to allow Plaintiff and the Nationwide Class to (i) take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their PII and PHI by third parties and (ii) prepare for the sharing and detrimental use of their confidential medical information.

117. Defendants had a duty to employ proper procedures to prevent the unauthorized dissemination of the PII and PHI of Plaintiff and the Nationwide Class.

118. Defendants have admitted that the PII and PHI of Plaintiff and the Nationwide Class was wrongfully lost and disclosed to unauthorized third persons as a result of the Data Breach.

119. Defendants, through their actions and/or omissions, unlawfully breached their duties to Plaintiff and the Nationwide Class by failing to implement industry protocols and exercise reasonable care in protecting and safeguarding the PII and PHI of Plaintiff and the Nationwide Class during the time the PII and PHI was within Defendants' possession or control.

120. Defendants improperly and inadequately safeguarded the PII and PHI of Plaintiff and the Nationwide Class in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

121. Defendants failed to heed industry warnings and alerts to provide adequate safeguards to protect the PII and PHI of Plaintiff and the Nationwide Class in the face of increased risk of theft.

122. Defendants, through their actions and/or omissions, unlawfully breached their duty to Plaintiff and the Nationwide Class by failing to have appropriate procedures in place to detect and prevent dissemination of the PII and PHI.

123. Defendants breached their duty to exercise appropriate clearinghouse practices by

failing to remove from the Internet-accessible environment any PII and PHI they were no longer required to retain pursuant to regulations and which Defendants had no reasonable need to maintain in an Internet-accessible environment.

124. Defendants, through their actions and/or omissions, unlawfully breached their duty to adequately and timely disclose to Plaintiff and the Nationwide Class the existence and scope of the Data Breach.

125. But for Defendants' wrongful and negligent breach of duties owed to Plaintiff and the Nationwide Class, the PII and PHI of Plaintiff and the Nationwide Class would not have been compromised.

126. There is a close causal connection between Defendants' failure to implement security measures to protect the PII and PHI of Plaintiff and the Nationwide Class and the harm, or risk of imminent harm, suffered by Plaintiff and the Nationwide Class. The PII and PHI of Plaintiff and the Nationwide Class was lost and accessed as the proximate result of Defendants' failure to exercise reasonable care in safeguarding such PII and PHI by adopting, implementing, and maintaining appropriate security measures.

127. As a direct and proximate result of Defendants' negligence, Plaintiff and the Nationwide Class have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity of how their PII and PHI is used; (iii) the compromise, publication, and/or theft of their PII and PHI; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII and PHI; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover

from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PII and PHI, which remain in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII and PHI of Plaintiff and the Nationwide Class; and (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII and PHI compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and the Nationwide Class.

128. As a direct and proximate result of Defendants' negligence, Plaintiff and the Nationwide Class have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

129. Additionally, as a direct and proximate result of Defendants' negligence, Plaintiff and the Nationwide Class have suffered and will suffer the continued risks of exposure of their PII and PHI, which remain in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII and PHI in its continued possession.

130. As a direct and proximate result of Defendants' negligence, Plaintiff and the Nationwide Class are entitled to recover actual, consequential, and nominal damages.

COUNT II
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiff and the RAAI Subclass and Against RAAI)

131. Plaintiff re-alleges and incorporate by reference herein all of the allegations contained in paragraphs 1 through 99.

132. In obtaining services from RAAI, Plaintiff and the RAAI Subclass provided and entrusted their PII and PHI to RAAI.

133. Defendants' website confirms that RAAI intended to bind itself to protect the PII and PHI that Plaintiff and the RAAI Subclass submitted to RAAI to obtain services.

134. RAAI required Plaintiff and the RAAI Subclass to provide and entrust their PII and PHI as condition of obtaining services from RAAI.

135. As a condition of obtaining services from RAAI, Plaintiff and the RAAI Subclass provided and entrusted their PII and PHI. In so doing, Plaintiff and the RAAI Subclass entered into implied contracts with RAAI by which RAAI agreed to safeguard and protect such PII and PHI, to keep such PII and PHI secure and confidential, and to timely and accurately notify Plaintiff and the RAAI Subclass if their PII and PHI had been compromised or stolen.

136. Plaintiff and the RAAI Subclass fully performed their obligations under the implied contracts with RAAI.

137. RAAI breached the implied contracts it made with Plaintiff and the RAAI Subclass by failing to implement appropriate technical and organizational security measures designed to protect their PII and PHI against accidental or unlawful unauthorized disclosure or unauthorized access and otherwise failing to safeguard and protect their PII and PHI and by failing to provide timely and accurate notice to them that PII and PHI was compromised as a result of the data breach.

138. As a direct and proximate result of RAAI's above-described breach of implied contract, Plaintiff and the RAAI Subclass have suffered (and will continue to suffer) the threat of the sharing and detrimental use of their confidential medical information; ongoing, imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and

economic harm; loss of the confidentiality of the stolen confidential data; the illegal sale of the compromised data on the dark web; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts, decreased credit scores and ratings; lost work time; and other economic and non-economic harm.

139. As a direct and proximate result of RAAI's above-described breach of implied contract, Plaintiff and the RAAI Subclass are entitled to recover actual, consequential, and nominal damages.

COUNT III
BREACH OF FIDUCIARY DUTY
(On Behalf of Plaintiff and the RAAI Subclass and Against RAAI)
(In the alternative to Count III)

140. Plaintiff re-alleges and incorporate by reference herein all of the allegations contained in paragraphs 1 through 99.

141. A relationship existed between Plaintiff and the RAAI Subclass and RAAI in which Plaintiff and the RAAI Subclass put their trust in RAAI to protect the private information of Plaintiff and the RAAI Subclass and RAAI accepted that trust and thereby gained a resulting superiority or influence over Plaintiff and the RAAI Subclass.

142. RAAI breached the fiduciary duty that it owed to Plaintiff and the RAAI Subclass by failing to act with the utmost good faith, fairness, and honesty, failing to act with the highest and finest loyalty, and failing to protect the private information of Plaintiff and the RAAI Subclass.

143. RAAI's breach of fiduciary duty was a legal cause of damage to Plaintiff and the RAAI Subclass.

144. But for RAAI's breach of fiduciary duty, the damage to Plaintiff and the RAAI Subclass would not have occurred.

145. RAAI's breach of fiduciary duty contributed substantially to producing the damage to Plaintiff and the RAAI Subclass.

146. As a direct and proximate result of RAAI's breach of fiduciary duty, Plaintiff and the RAAI Subclass are entitled to and demand actual, consequential, and nominal damages and injunctive relief.

COUNT IV
AIDING AND ABETTING BREACH OF FIDUCIARY DUTY
(On Behalf of Plaintiff and the RAAI Subclass and Against Somnia)
(In the alternative to Count III)

147. Plaintiff re-alleges and incorporate by reference herein all of the allegations contained in paragraphs 1 through 99.

148. A relationship existed between Plaintiff and the RAAI Subclass and RAAI in which Plaintiff and the RAAI Subclass put their trust in RAAI to protect the private information of Plaintiff and the RAAI Subclass and RAAI accepted that trust and thereby gained a resulting superiority or influence over Plaintiff and the RAAI Subclass.

149. RAAI breached the fiduciary duty that it owed to Plaintiff and the RAAI Subclass by failing to act with the utmost good faith, fairness, and honesty, failing to act with the highest and finest loyalty, and failing to protect the private information of Plaintiff and the RAAI Subclass.

150. RAAI's breach of fiduciary duty was a legal cause of damage to Plaintiff and the RAAI Subclass.

151. But for RAAI's breach of fiduciary duty, the damage to Plaintiff and the RAAI Subclass would not have occurred.

152. RAAI's breach of fiduciary duty contributed substantially to producing the damage to Plaintiff and the RAAI Subclass.

153. Somnia induced or participated in RAAI's breach of fiduciary duty by failing to implement appropriate safeguards to protect the Plaintiff's and the RAAI Subclass's PII and PHI.

154. As a direct and proximate result of RAAI's breach of fiduciary duty, Plaintiff and the RAAI Subclass are entitled to and demand actual, consequential, and nominal damages and injunctive relief.

COUNT V
Declaratory Judgment
(On Behalf of Plaintiff and the Nationwide Class)

155. Plaintiff re-alleges and incorporate by reference herein all of the allegations contained in paragraphs 1 through 99.

156. Under the Declaratory Judgment Act, 28 U.S.C. § 2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Further, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described in this Complaint.

157. An actual controversy has arisen in the wake of the Data Breach regarding Plaintiff's and Class Members' PII and PHI and whether Defendants are currently maintaining data security measures adequate to protect Plaintiff and Class Members from further data breaches that compromise their PII and PHI. Plaintiff alleges that Defendants' data security measures remain inadequate. Defendants publicly deny these allegations. Furthermore, Plaintiff continue to suffer injury as a result of the compromise of their PII and PHI and remains at imminent risk that further compromises of their PII and PHI will occur in the future. It is unknown what specific measures and changes Defendants have undertaken in response to the Data Breach.

158. Plaintiff and Class Members have an ongoing, actionable dispute arising out of Defendants' inadequate security measures, including (i) Defendants' failure to encrypt Plaintiff's

and Class Members' PII and PHI, including Social Security numbers, while storing it in an Internet-accessible environment and (ii) Defendants' failure to delete PII and PHI they have no reasonable need to maintain in an Internet-accessible environment.

159. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Defendants owe a legal duty to secure the PII and PHI of past and current patients of Defendants and their affiliates;

b. Defendants continue to breach this legal duty by failing to employ reasonable measures to secure consumers' PII and PHI; and

c. Defendants' ongoing breaches of their legal duty continue to cause Plaintiff harm.

160. This Court also should issue corresponding prospective injunctive relief requiring Defendants to employ adequate security protocols consistent with law and industry and government regulatory standards to protect consumers' PII and PHI. Specifically, this injunction should, among other things, direct Defendants to:

d. engage third party auditors, consistent with industry standards, to test their systems for weakness and upgrade any such weakness found;

e. audit, test, and train their data security personnel regarding any new or modified procedures and how to respond to a data breach;

f. regularly test their systems for security vulnerabilities, consistent with industry standards;

g. implement an education and training program for appropriate employees regarding cybersecurity.

161. If an injunction is not issued, Plaintiff will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach at Defendant. The risk of another such breach is real, immediate, and substantial. If another breach at Defendants occurs, Plaintiff will not have an adequate remedy at law because many of the resulting injuries are not readily quantified and they will be forced to bring multiple lawsuits to rectify the same conduct.

162. The hardship to Plaintiff if an injunction is not issued exceeds the hardship to Defendants if an injunction is issued. Plaintiff will likely be subjected to substantial identity theft and other damage. On the other hand, the cost to Defendants of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Defendants have a pre-existing legal obligation to employ such measures.

163. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach at Defendants, thus eliminating the additional injuries that would result to Plaintiff and others whose confidential information would be further compromised.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself and Class Members, requests judgment against Defendants and that the Court grant the following:

A. For an Order certifying the Nationwide Class and the RAAI Subclass and appointing Plaintiff and his Counsel to represent each such Class;

B. For equitable relief enjoining Defendants from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of the PII and PHI of Plaintiff and Class Members, and from refusing to issue prompt, complete, any accurate disclosures to Plaintiff and Class Members;

C. For injunctive relief requested by Plaintiff, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class Members, including but not limited to an order:

i. prohibiting Defendants from engaging in the wrongful and unlawful acts described herein;

ii. requiring Defendants to protect, including through encryption, all data collected through the course of their business in accordance with all applicable regulations, industry standards, and federal, state or local laws;

iii. requiring Defendants to delete, destroy, and purge the personal identifying information of Plaintiff and Class Members unless Defendants can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members;

iv. requiring Defendants to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the PII and PHI of Plaintiff and Class Members;

v. prohibiting Defendants from maintaining the PII and PHI of Plaintiff and Class Members on a cloud-based database;

vi. requiring Defendants to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendants' systems on a periodic basis, and ordering Defendants to promptly correct any problems or issues detected by such third-party security auditors;

vii. requiring Defendants to engage independent third-party security auditors and

internal personnel to run automated security monitoring;

viii. requiring Defendants to audit, test, and train their security personnel regarding any new or modified procedures;

ix. requiring Defendants to segment data by, among other things, creating firewalls and access controls so that if one area of Defendants' network is compromised, hackers cannot gain access to other portions of Defendants' systems;

x. requiring Defendants to conduct regular database scanning and securing checks;

xi. requiring Defendants to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiff and Class Members;

xii. requiring Defendants to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xiii. requiring Defendants to implement a system of tests to assess their respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees compliance with Defendants' policies, programs, and systems for protecting personal identifying information;

xiv. requiring Defendants to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendants' information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xv. requiring Defendants to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves;

xvi. requiring Defendants to implement logging and monitoring programs sufficient to track traffic to and from Defendants' servers; and for a period of 10 years, appointing a qualified and independent third party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendants' compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment;

D. For an award of damages, including actual, consequential, and nominal damages, as allowed by law in an amount to be determined;

E. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

F. For prejudgment interest on all amounts awarded; and

G. Such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff hereby demands that this matter be tried before a jury.

Date: November 11, 2022

Respectfully Submitted,

/s/ Jonathan M. Sedgh
Jonathan M. Sedgh
MORGAN & MORGAN
850 3rd Ave, Suite 402
Brooklyn, NY 11232
Phone: (212) 738-6839
Fax: (813) 222-2439
Email:jsedgh@forthepeople.com

John A. Yanchunis*
Ryan D. Maxey*
MORGAN & MORGAN COMPLEX BUSINESS DIVISION
201 N. Franklin Street, 7th Floor
Tampa, Florida 33602
(813) 223-5505
jyanchunis@ForThePeople.com
rmaxey@ForThePeople.com

Attorneys for Plaintiff and the Proposed Class

**pro hac vice applications pending*

CERTIFICATE OF SERVICE

I hereby certify that on November 11, 2022, the foregoing document was filed with the Clerk by using the CM/ECF system, which will send notification to all attorneys of record in this matter.

/s/ Jonathan M. Sedgh
Jonathan M. Sedgh
MORGAN & MORGAN
850 3rd Ave, Suite 402
Brooklyn, NY 11232
Phone: (212) 738-6839
Fax: (813) 222-2439
Email:jsedgh@forthepeople.com